Paradigm Academic Press
Law and Economy
ISSN 2788-7049
JUL. 2024 VOL.3, NO.7

Challenges and Prospects for the Law of Armed Conflict — A Humanitarian Perspective

Wenting Ouyang[1]

[1] Law School, Beijing Normal University, Beijing, China

Correspondence: Wenting Ouyang, Law School, Beijing Normal University, Beijing, China.

doi:10.56397/LE.2024.07.06

Abstract

The law of armed conflict, as the international legal system that regulates the conduct of war and mitigates its catastrophic consequences, has in recent years faced the challenges of high-tech forms of warfare, the involvement of non-state actors, and the complexities of civil-military integration. To address the complexity of non-international armed conflict, international humanitarian law should be "strategically" disseminated, non-government parties should be urged to issue unilateral declarations or codes of conduct, and the UN Security Council Action Plan model and the Geneva Call's "Deed of Commitment" model should continue to be explored and implemented. The distinction between combatants and civilians in cyber-armed conflict requires more attention to actual behavior than to the appearance of the operator, with full consideration of the relationship between full membership and function. For the use of autonomous weapons systems, we must balance military interests and the consequences of damage, maximize the recognition and decision-making capabilities of autonomous weapons systems, and maintain human oversight and control during high-risk decisions.

Keywords: armed conflict, humanitarian, principle of distinction, autonomous weapons systems

1. Introduction

Taking stock of the wars and conflicts that will be raging across the globe in 2023, UN Secretary-General António Guterres said with concern: "Conflicts are becoming more complex, more deadly, and more difficult to resolve… New potential areas of conflict and weapons of war are creating new ways human beings can self-destruct." The Law of Armed Conflict (LOAC) is designed to regulate the "minimum" civilized standards needed to mitigate the scourge of war, the most uncivilized act of human insanity. However, in recent years, the high-tech nature of warfare, the involvement of non-state military actors, and the difficulty of distinguishing between civilian and military objectives have all contributed to the humanitarian challenges of armed conflict.

2. Law of Armed Conflict and Humanitarian Protection

The law of armed conflict, i.e., international humanitarian law, has developed and evolved in its vein over more than 150 years of history and several phases. In the course of its development, the Geneva system and the Hague system of law were formed. The current Geneva Conventions system consists of four Geneva Conventions and two Additional Protocols. The Additional Protocols contain many of the rules of the Hague system in the original terminology of the laws of war, and thus the contents of the two systems are combined to form the present IHL. These rules are to be observed by belligerents or parties to a conflict in the event of war or armed conflict between them.

Among the many principles of the law of armed conflict, the principle of the protection of humanity concerns the purpose, the overall situation, and the direction of development of the law of armed conflict and is universally applicable to all legal relations in this field and governs its development. The basic meaning of the principle of

humane protection is that combatants in armed conflict enjoy universal protection from the effects of hostilities; they must be respected, protected, and treated humanely. In other words, it prohibits the infliction of injuries, damage, and suffering that are not necessary to deprive the enemy of resistance; and it respects, protects, and relieves the victims of armed conflict. The humanitarian principle was first mentioned in the "Martens Clause" of the Hague Convention No. 2 of 1899 and then recurred in the Geneva Conventions of 1949 and the two Additional Protocols of 1977. It is considered a fundamental principle of the law of armed conflict mainly because of the inevitability of war and armed conflict, the requirements of human nature, and the rational choice of human beings under conditions of helplessness about war or armed conflict.

"War in all ages has its peculiar limitations and scope." In contemporary armed conflicts, the boundaries between military and civilians are gradually blurring or even disappearing; drones and autonomous weapons systems have made it unnecessary for some soldiers to fight in battle, and the destructive power of war has been greatly increased; cyber-attacks are capable of inflicting unprecedented threats and damages on nations, challenging international law and providing it with a vast space for change and a powerful driving force.

3. Subject: Dispute Arising out of a Non-International Armed Conflict

3.1 Difficulties in Complying with Humanitarian Law in Non-International Armed Conflicts

The application of the law of armed conflict has undergone profound changes in recent years as armed conflicts have continued. Initially, the law of armed conflict was adjusted to the conduct of war between States, as exemplified by the Geneva Conventions and Additional Protocol I. The law of armed conflict is not a matter of military force but of reciprocal obligations and rights. After World War II, the laws of war began to regulate non-international armed conflicts. On the one hand, non-international armed groups did not participate in the drafting of the Geneva Conventions and Protocols and themselves lack a sense of belonging to the NHL, and states in conflict with such groups will of course strenuously oppose their participation in the discussion of the Conventions. For non-state subjects, not having participated in the formulation and development of the laws of war, but being required to comply with their implementation is undoubtedly an imposed burden, the benefits of which outweigh the costs, and which inevitably creates problems. On the other hand, the formation of rules of customary international humanitarian law has not emphasized non-state armed groups. In its study on Customary IHL, the International Committee of the Red Cross, in demonstrating that specific rules became customary international law, listed "treaties and other documents" and "State practice". "Other practice" is the last of the materials listed, which includes the practice of various non-State subjects, including non-State armed groups. In terms of the importance of the reference, it is less important than the practice of States. In addition, the protocol requires armed groups to have "effective control over a part of the territory" and to be "capable of conducting sustained and coordinated military operations". In reality, many armed groups are unable to meet such high standards, and the existing rules of the protocol are not yet complete.

3.2 Promotion of Compliance with Humanitarian Law by Non-International Subjects

Firstly, following traditional approaches, IHL should be disseminated "strategically," encouraging non-state actors to issue unilateral declarations or codes of conduct to comply with IHL. Conflict states can be encouraged to spread knowledge of IHL among civilians, allowing the public to access legal documents in their national language. This helps non-state actors understand the relationship between IHL and military benefits, realizing that adherence to humanitarian law aligns with common interests and deepens recognition of IHL. The traditional methods for complying with IHL primarily include special agreements, unilateral declarations, codes of conduct, and ceasefire or peace agreements. Common Article 3 of the Geneva Conventions encourages parties to non-international armed conflicts to implement more effectively the provisions of international humanitarian law by concluding special agreements. As armed groups have become more frequently involved in contemporary armed conflicts, the status of such agreements as a means of enhancing parties' compliance with international humanitarian law has increased. The decision-making process for special agreements recognizes that all parties to a conflict are involved in clarifying and expanding applicable rights and obligations in a manner that is consistent with the principle of equality of belligerents and provides incentives for armed groups to respect international humanitarian law that they have negotiated. Non-state armed groups have long issued unilateral declarations expressing their willingness to comply with humanitarian law, a relatively easier and more common practice. However, due to political influences and the abstract nature of these declarations, the actual likelihood of adherence or successful fulfillment is not very high. Codes of conduct for non-state armed groups are more practical because they entail implementing specific IHL rules. Furthermore, when the leadership of armed groups actively formulates or endorses a code of conduct, it indicates their recognition and commitment to ensuring compliance. Compared to rules perceived as externally imposed, adhering to and implementing "their own" rules is more likely to influence the behavior of armed group members.

Secondly, there is the United Nations Security Council action plan model between "unequal entities." This approach involves the UN and the armed United Nations Security Council taking sanctions to ensure non-state

armed groups implement the action plan and comply with IHL. The protection scope of the Security Council action plan in armed conflicts primarily includes protecting children's rights, particularly prohibiting the recruitment and use of child soldiers, and safeguarding the safety of women and girls by combating sexual violence. Regarding child soldiers, the Security Council has passed a series of resolutions, especially the four Geneva Conventions and the United Nations Convention on the Rights of the Child, and established an early monitoring group, requiring the Secretary-General to report annually on the implementation of child protection. For non-compliant armed groups, measures include restricting military equipment exports and sanctioning relevant leaders. For women and girls, the United Nations has adopted several resolutions and international treaties, calling on parties to armed conflict to take special measures to protect women from gender-based violence, particularly rape and other forms of sexual abuse. Despite the action plan model having corresponding safeguards, some armed groups have long overstepped their bounds and been added to blacklists, and the effects of sanctions are not perfect.

Thirdly, there is the "Geneva Call" commitment model between "equal entities," which involves contact between non-governmental organizations, other civil society groups, individuals, and non-state armed groups. Founded in 2000 and based in Geneva, Switzerland, Geneva Call is a non-governmental organization aimed at increasing "armed non-state actors'" respect for IHL and enhancing the protection of civilians in armed conflicts. The basic content of its "commitment letter" model is to select the most promising armed non-state actors for positive humanitarian impact on civilian protection and engage with them. Through frequent contact and training on IHL norms, these actors' "awareness of international humanitarian norms is raised, and they are convinced of the value of adhering to these norms." Once the timing is right, non-state armed groups can use commitment letters, unilateral declarations, internal rules and regulations, bilateral or multilateral agreements, etc., to express their willingness to comply with IHL norms. Geneva Call, although limited in scope, has been able to sign a large number of commitment letters with non-state armed groups, including specific positive and negative obligations of the actors. The Geneva Call could therefore focus on its role as a neutral and independent mediator, committed to maintaining a dialogue with all those involved in the war or influencing the conduct of the war, listening to the parties to the armed conflict rather than simply telling them what to do, and helping to establish or restore a minimum level of trust. relationship of trust and, most importantly, to allow the Geneva Call to monitor compliance. Currently, the "letter of commitment" model has made some progress in banning anti-personnel landmines, and sexual violence, protecting children in armed conflict, and protecting medical personnel, but its effectiveness remains to be seen in the long term as it does not have a mandatory mechanism to ensure implementation.

4. Space: Cyber Armed Conflict Under Civil-Military Integration

4.1 Cyber Armed Conflict Poses a Unique Threat

After the Second World War, countries around the world shifted their focus to economic construction and adopted a strategy based on economic and technological competition, supplemented by competition in military power, which facilitated the tremendous development of shared civilian and military technologies and the formation of their own models of civil-military integration and development. From the perspective of pursuing national development, the effects of the civil-military integration policy have been remarkable, and the accompanying change in armed conflict is that battlefields in the traditional physical sense are disappearing, and impacts are beginning to be carried out digitally in virtual space by storing, modifying and exchanging data through cyber infrastructures. Extremists, organized crime, and hegemonic states also seek new hegemony or increased influence through cyber. According to the 2013 Tallinn Manual on the International Law of Cyber Warfare, a cyber attack is "an offensive or defensive cyber action that can reasonably be foreseen to result in the injury or death of persons, damage to or destruction of objects." Cyber-armed conflict may pose a unique threat to international security. First, the blurring of the civil-military nature of the subject of confrontation. From cold wars, thermonuclear wars, and mechanized wars, dedicated standing armies have been the most common mode of combat in modern civilized societies. Nowadays, with the widespread need for cutting-edge technology in the military, soldiers with only ordinary computer knowledge can no longer meet combat needs, and the troops have to hire or borrow a large number of employees and experts from companies that master high technology to serve the military forces. In this way, the distinction between civilians and combatants in cyberattacks has been eroded. Second, it is difficult to distinguish between the objects of cyber attacks. Unlike traditional kinetic strikes, due to the interoperability of cyberspace and the high degree of integration of civilian and military networks, it may be impossible to distinguish which part of the network is or will be used for military information or operational transmission, which means that all civilian objects in cyberspace may become military targets and the geographic boundaries of armed conflict become a fundamental issue. Thirdly, the criteria for determining "direct participation in hostilities" are not clear. Regarding direct participation in hostilities, the ICRC Interpretative Guidelines set out three criteria: "threshold of damage", "direct causation" and "belligerent link", and also the time frame was examined. It is worth exploring how combatant status in real life can be mapped to

cyberspace, and to what extent the involvement of non-military technicians in computer network attacks can lead to a finding of "direct participation" in hostilities and a loss of civilian protection.

4.2 Approaches to the Application of the Principle of Distinction

The principle of distinction, as the "overarching principle" of international humanitarian law, mandates that parties in an armed conflict must differentiate between combatants and non-combatants, between armed forces and civilians, and between military and non-military objectives. On one hand, the principle of distinction embodies the protection of non-combatants and civilian objects, and on the other hand, it provides economic and lawful means for the warring parties to achieve their military objectives, which is significant in guiding the lawful conduct of war and minimizing civilian casualties. In contextualizing the discussion on the applicability of the principle of distinction, attention should be given to the position of the ICRC in this field. The position of the ICRC, which is engaged in humanitarian assistance activities on the front lines of current armed conflicts of all kinds, is in line with the broader humanitarian protection position and is now beginning to play a role in exploring ways to constrain the indiscriminate use of cyber attacks by both governmental armed forces and organized armed groups. Supporting the International Committee of the Red Cross in expressing its views in relevant multilateral contexts is conducive to the realization of humanitarian protection values such as the principle of distinction. In addition, the views of other international organizations on this issue should, as far as possible, be compatible with the basic thrust pursued by the ICRC, and the issue should be discussed in the sense of enhancing humanitarian protection rather than armed conflict.

Regarding the distinction between combatants and civilians in cyber attacks, cyber combatants are combatants taking part in cyber hostilities in the context of cyber warfare, and cyber combatants of armed forces or other militias or other voluntary forces. By Article 4(1)(b) of the Third Geneva Convention and customary international law, members of other militias and other voluntary forces are required to meet the following conditions: (1) to be under the command of a person who is responsible for his/her subordinates; (2) to have a fixed distinctive emblem that can be recognized from a distance; (3) to carry arms openly; and (4) to fight in compliance with the laws of armed conflict. Elements (2) and (3) are formal elements, that are more difficult to apply directly in cyberspace, and the actual effect may be deviated, so some adaptations are needed. The traditional combatant criteria of whether the operator is wearing a uniform, wearing a cyber combatant symbol, or possessing a weapon can no longer be applied universally. Even when attempting to trace an IP address to whether it is in a military zone, the IP address can be spoofed or proxied through layers, and the result of the trace may not be the true source of the attack launch. For element (2), the Tallinn Manual Version 2.0 recognizes that cyber combatants do not need to comply with this at all times, and only applies when the failure to wear fixed distinctive markings may result in an attacker's inability to distinguish between a civilian and a combatant, and therefore puts the civilian at greater risk of being mistakenly attacked. Elements (1)(4) are substantive elements, which require more attention to actual behavior than to the appearance of the operator, with due regard to the relationship between full membership and function. In practical application, the individual needs to be analyzed in the context of the specific situation. For example, the scope of the combatant of "attackability" is limited to the existence of such targets to the military activities of the real contribution, and such targets have irreplaceable military interests. Combatants often belong to organized armed forces, groups, and units, are subject to internal disciplinary constraints, and have commanders in charge. In general, sporadic, spontaneous, and unorganized participation in direct hostilities should still be considered civilian. However, for other militia and volunteer force elements in cyber warfare, the need to be organized is debatable. With advances in cyber ICT, one or a few cyber combatants can launch a devastating cyber attack against a target, so even individual or relatively loosely organized cyber operations have the potential to reach a high level of violence. This matter can be addressed by examining the relationship between the fragmented combatant and the party to the conflict to which he or she belongs. If a party to the conflict exercises control over a cyber-combatant beyond the mere provision of economic, armament, or training support, even if the combatant or the loosely organized group to which he or she belongs does not meet the criterion of organization, his or her actions may be attributed to the State or corresponding group because they satisfy the requirement of "overall control".

Regarding the distinction between targets in cyber attacks, some scholars advocate for the concepts of "infrastructure immunity from attack" and "essential civilian functions." However, the definitions of critical infrastructure and essential civilian functions are often vague, and segregating military and civilian networks is also unrealistic. The "attack ability" of dual-use targets in a cyber-armed conflict should be limited to the existence of a realistic contribution of such targets to military activities and the irreplaceable military advantage of such targets. Since there is no single form of organized cyber attack, the above determination needs to be made on a case-by-case basis, judging the legitimacy of the attack from the overall process of each case. If there is no "realistic contribution and irreplaceability", the attack on the target is not sufficiently justified. This criterion is more suited to adjudicative rather than behavioral standards, but it can make a difference in terms of humanitarian protection if it causes concern on both sides of the conflict. In terms of a standard of conduct, a

feasible idea at present is that a State can partially make a clear distinction between its civilian and military targets and that the State needs to make it clear in the cyber environment which targets belong to the civilian sphere, i.e., through the establishment of a "digital security zone", to ensure that civilian targets will not be attacked in the event of a cyber-armed conflict. Other states should respect the establishment of these "digital security zones" and commit to not attacking these designated targets. The initiator of a cyber attack should ascertain, each time an attack is launched, whether the cyber weapon used is capable of actually being directed at the intended target in the circumstances, taking fully into account the issue of "targeting" in the context of civil-military integration. In particular, attackers should not use cyber weapons that are by their nature indistinguishable from their targets, and the application of such weapons should be prohibited during their development or review, such as viruses that are capable of replicating themselves and are impossible to control. This approach helps protect non-military targets from cyber threats and maintains cyber security and international peace and stability. Ultimately, what constitutes a "clear, concrete, and direct military advantage" and a "tangible contribution to military activities" in the context of cyber warfare must be determined by governments.

The criterion of direct participation in hostilities is crucial for determining whether civilians become legitimate targets in cyber attacks. A person directly participates in hostilities when their conduct aims to support one side of the conflict to the detriment of the other by causing death, injury, or destruction, or by directly undermining the enemy's military operations or strength. When civilians engage in or assist with such acts, they lose their protection from attack. Non-military technicians can be considered to be taking a "direct part in hostilities" if they: (1) Initiate a cyber attack against a specific target, knowingly conduct a cyber attack on key aspects such as critical infrastructure, government agencies, or military systems; or (2) Assist in planning and executing cyber attacks, providing technical support, guidance, or assistance. There must be a direct causal relationship between the cyber attacks conducted by the perpetrator and the resulting damage. Indirect contributions, such as the design and maintenance of computer programs not directly linked to a specific military cyber attack, do not constitute direct participation in hostilities.

5. Object: Ethical and Technological Challenges of Autonomous Weapons Systems

5.1 Technical Limitations of Autonomous Weapons Systems in Armed Conflict

According to the U.S. Department of Defense's definition of an autonomous weapon system (AWS), an AWS is a weapon system that, once activated, can select and attack a target without further intervention by a human operator, including human-supervised autonomous weapon systems designed to allow a human operator to deactivate the weapon system, and to select and attack a target without further intervention after activation. AWS has the emergence of AWS poses several key challenges to contemporary armed conflict. First, even state-of-the-art AI technology is currently unable to guarantee the correct distinction in all contexts, especially in complex and dynamic battlefield environments, which can lead to unnecessary civilian casualties and property destruction. Secondly, the relationship between balancing military advantage and civilian casualties is extremely complex and may not be fully understood and assessed by AI, and there is uncertainty as to whether the principle of necessity can be strictly adhered to when deciding on the use of force. Third, even if autonomous weapons systems are designed to allow human operators to intervene, the ability to intervene promptly during actual operation remains problematic. If a weapon system is hacked or suffers a technical malfunction, this could lead to uncontrollable consequences. Fourth, autonomous weapons systems may lack the empathy and ethical judgment to treat wounded combatants or captured enemy soldiers appropriately, potentially weakening the principle of humane treatment. Fifth, IHL has weak enforcement mechanisms for restricting methods and means of warfare in wars and armed conflicts, which are often facilitated through ex post facto accountability.

5.2 Development and Use of Technologies for Absolute Human Control of AI Weapons

Autonomous weapons systems raise significant issues concerning the principles of distinction, predictability, and humane treatment, requiring nuanced discretion for specific scenarios, which remains a technically complex matter. One scholar highlights the ideal scenario where "if biological information about individual targets is combined with the battlefield, the distinction will rise to unprecedented levels." However, this ideal scenario is still speculative; for the foreseeable future, the ability of autonomous weapons systems to distinguish between combatants and civilians cannot be solely determined by numbers and parameters. Human cognition and reasoning remain essential for assessing and responding to ambiguities. Nevertheless, efforts should be made to ensure that AI operations adhere to normative standards.

The international community might consider establishing an international supervisory body to oversee the development and use of autonomous weapons systems, promoting the harmonization of relevant standards and norms through enhanced international cooperation and the sharing of technology and operational experience. States should establish clear legal standards and submit regular reports to this monitoring body. These standards should encompass technical requirements and operational norms, such as target identification accuracy,

situational analysis capability, and performance in complex battlefield environments. Before deploying autonomous weapons systems, they must undergo rigorous testing and verification to continually refine their ability to accurately distinguish between civilians and combatants, as well as civilian objects and military targets, in various complex and dynamic battlefield scenarios. There should be a commitment to improving the recognition and decision-making capabilities of these systems to minimize the risk of miscalculation and accidental injury. All personnel involved in the development, testing, deployment, and use of autonomous weapons systems must undergo comprehensive training in international humanitarian law and obtain appropriate certification. This training should cover the specific requirements of the principle of distinction, the importance of civilian protection, and the operation of autonomous weapons systems in complex battlefield environments to prevent indiscriminate killings. The international supervisory body should regularly review the autonomous weapons systems of different states to ensure they remain under human control and comply with international humanitarian law. Relevant international legal frameworks and technical standards should be regularly assessed and updated to keep pace with advancements in AI technologies and changes in battlefield environments.

The principle of proportionality involves subjective judgment, balancing incidental civilian harm against anticipated or direct military benefits. Battlefield conditions change rapidly, and military benefits can vary over time and among different commanders, making precise comparisons difficult. Decisions regarding proportionality are inherently qualitative and cannot be quantified with precision. Autonomous weapons systems should be evaluated based on real-time, reliable information and in line with the principle of proportionality as understood by a reasonable human being, without demanding ex post facto evaluations. Improvements to autonomous weapons systems should focus on embedding the principle of proportionality into decision-making algorithms; acquiring and analyzing real-time battlefield data by integrating with other battlefield systems; using advanced sensors and AI technologies to enhance target identification accuracy and battlefield situational awareness; and maintaining human oversight and control, especially when there is a high risk of excessive civilian casualties. The system should alert human operators for final decision-making in such scenarios. Preliminary military benefit assessments can be conducted based on preset rules and scenarios, which should be regularly updated and adjusted based on experience and new intelligence to ensure consistency with real battlefield conditions.

Finally, it is necessary to establish and improve oversight mechanisms for the use of autonomous weapons systems. From a practical perspective, IHL primarily serves to protect the legitimate rights of war victims during wars or armed conflicts, with such protection largely provided by the ICRC and other non-governmental international organizations. However, when it comes to the selection of combat methods and means by parties in a war or armed conflict, including the use of high-tech weapons that may not conform to IHL principles such as distinction and the avoidance of unnecessary suffering, impartial and neutral humanitarian organizations and Protecting Powers under the IHL framework have only limited advisory and critical capacities, lacking actual enforcement authority. This limitation does not effectively constrain the methods and means of warfare. Chapter VII of the United Nations Charter stipulates that the primary responsibility of the United Nations Security Council (UNSC) is to maintain international peace and security. The UNSC holds a paramount political position within the UN system and is the only body authorized to undertake non-military and military actions to maintain international peace and security. Therefore, during wars or armed conflicts, the role of the UNSC should be fully leveraged to establish an authoritative IHL oversight body. This body, utilizing the UNSC's primary political standing, should ensure the effective legal regulation of warfare methods and means through real-time oversight. Moreover, the UNSC should condemn parties in wars or armed conflicts that use high-tech weapons in violation of IHL and exert corresponding political and legal pressure, including imposing appropriate sanctions. Only by actively playing its role can the UNSC effectively address the current gap in real-time oversight under international humanitarian law.

6. Conclusion

The law of armed conflict, as an important component of international humanitarian law, is faced with the challenge of increasingly complex and volatile patterns of warfare. The rise of non-state armed groups and the emergence of cyber warfare, as well as the application of high-tech tools of war, such as drones and autonomous weapons systems, have dramatically altered the traditional modes of warfare and put the current legal system to a severe test.

For non-international armed conflict participants, in order to better protect civilians in conflicts, the international community should strengthen communication with non-state armed groups, raise their awareness and recognition of humanitarian law through practical actions, and urge non-state actors to abide by humanitarian law through various forms of agreements, declarations, and codes of conduct. In the context of cyber armed conflict, in addition to appearance or identity markers, the operator's behavior and contribution to the military activity is the key to distinguishing between combatants and civilians, military targets and non-military targets.

In the case of targets, States may consider establishing “digital safe zones” to protect civilian infrastructure. For the use of autonomous weapons systems, we must find a balance between military interests and ethical scrutiny. Even though autonomous weapons systems have made significant technological progress, their practical application in battlefield environments still requires caution to ensure that human beings have absolute control over the technological development and use of AI weapons. In conclusion, in the face of the challenges of armed conflict in the new era, it is only through the efforts of many parties to jointly safeguard and promote the development of international humanitarian law that human dignity can be better protected. Then lasting peace realized.

References

Christopher P. Toscano, (2015). Friend of Humans: An Argument for Developing Autonomous Weapons Systems. *Journal of National Security Law and Policy*, *8*, pp. 207-208.

Erie Boylan, (2017). Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners. *Vanderbilt Journal of Transnational Law*, *50*, p. 232.

Ido Kilovaty, (2017). ICRC, NATO and the U.S. Direct Participation in Hacktivities Targeting Private Contractors and Civilians in Cyberspace under International Humanitarian Law. *Duke Law & Technology Review*, *15*, pp. 1-38.

James Emory Jr. Tucker, (2017). The Targeting of Non-State-Affiliated Civilians in Cyberspace: Lagging LOAC Principles Cause Uncertainty on Both Sides. *North Carolina Journal of International Law*, *42*, pp. 1036-1037.

Kenneth Anderson, Daniel Reisner and Matthew Waxman, (2014). Adapting the Law of Armed Conflict to Autonomous Weapon Systems. *International Law Studies*, *90*, pp. 402-403.

Margaret T. Artz, (2012). Chink in the Armor: How a Uniform Approach to Proportionality Analysis Can End the Use of Human Shields. *Vanderbilt Journal of Transnational Law*, *45*, pp. 1447-1487.

Michael A. Newton, (2015). Back to the Future: Reflections on the Advent of Autonomous Weapons System. *Case Western Reserve Journal of International Law*, *47*, p. 21.

Michael N. Schmitt and Jeffrey S. Thurnher, (2013). Out of the Loop: Autonomous Weapon Systems and the Law of Armed Conflict. *Harvard National Security Journal*, *4*, pp. 262-265.

Michael N. Schmitt, (2014). The Law of Cyber Warfare: Quo Vadis. *Stanford Law & Policy Review*, *25*, p. 296.

Robin Geib and Henning Lahmann, (2012). Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. *Israel Law Review*, *45*, p. 389.

Theodor Meron, (2000). The Humanization of Humanitarian Law. *American Journal of International Law*, *94*, pp. 239-278.

Yoram Dinstein, (2012). The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict and Security Law*, *17*, p. 276.

Copyrights